REMARKS / ARGUMENTS

In response to the Office Action mailed February 17, 2005 ("the Office Action"), Applicants respectfully request that the Office enter the amendments set forth above and consider the following remarks. By this response, claims 11 and 18 are amended to correct minor and obvious typographical errors, and no claims have been canceled or added. After entry of this paper, claims 1-20 will remain pending in this application.

Rejection of Claims 1-20 under 35 U.S.C. § 103(a)

Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,754,829 to Butt et al. ("the '829 patent") in view of U.S. Patent No. 5,958,050 to Griffin et al. ("the '050 patent"). The rejections are traversed respectfully in view of the following remarks.

Embodiments of the present invention provide methods and systems to control access to computing resources with improved efficiency. Briefly, embodiments of the present invention determine whether a request for system resources should be granted by identifying the authorizations, certificates, and associated authorized principals necessary to securely grant or deny the request. Specification at paragraph [0037]. A "principal" is an entity that can make or authorize a request, and an authorization (or certificate) is an expression of the permissions granted by a principal. Specification at paragraph [0042]. Each of the authorizations (or certificates) is interpreted as a function of the state of one or more of the principals. Specification at paragraph [0037]. Processing logic iteratively evaluates these functions and updates the states of the principals to determine whether the request should be granted or denied. *Id.* In one embodiment, the certificates are evaluated until the state of the root authority indicates that the request should be granted or until further evaluation of the certificates is ineffective in changing the state of the principals, *i.e.,* a fixpoint is reached.

Some or all of these unique features and aspects are recited in the pending claims, as summarized below.

Claims 1–8 include at least the following unique elements: identifying a set of principals associated with a group of certificates; initializing a state associated with each principal; evaluating a certificate at least partly as a function of the state associated with one or more of the principals; updating the state of one or more of the principals if the result of the evaluation indicates that the state of a principal should be changed; and repeating such evaluating and updating until a fixpoint is reached or until a predefined principal is found to authorize the request.

Claim 9 includes at least the following unique elements: means for identifying a root principal from whom authorization is needed in order to grant a request; means for performing at least a portion of a least fixpoint computation over certificates to determine whether the root principal has authorized the requesting principal to access the piece of electronic content or processing resource; and means for granting access to the electronic content or processing resource if the least fixpoint computation indicates that the root principal has authorized such access.

Claims 10–16 include at least the unique element of a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by performing least fixpoint computations using digital certificates.

Claims 17–20 include at least the following unique elements: expressing authorizations using a structure that satisfies certain predefined properties; expressing each certificate as a function, wherein each function possesses one or more properties sufficient to ensure that a set of authorizations will have a fixpoint; computing a fixpoint of the authorizations, or an approximation thereof; and making a trust management decision using the result of such computations.

The '829 Patent

The '829 patent describes systems that allow an operator to control multiple devices having different operating systems from a console using a certificate-based authentication scheme.'829 patent at Column 3, lines 4–7. The '829 patent discloses "[a]n operating system independent method for an operator of a console to manage a device" in which "[a]n operating system independent session certificate is obtained by the operator of the console executing a first operating system, from a trusted core of the device executing a second operating system, to authenticate identity and group membership of the operator." *Id.* at Column 2, lines 26–34. Generally, "[t]he operating system independent session certificate is provided by the operator to the device executing a third operating system, along with a management request. . . . the device determines whether the authenticated operator has necessary access privilege to perform the management request based at least in part on the authenticated group membership of the operator set forth in the operating system independent session certificate." *Id.* at lines 36–40.

According to one example, validation of the operator is accomplished by determining whether the operator possesses a private key associated with a session certificate that is created when the operator logs-in to the "core" (the part of the system that controls access privileges) using the console. *Id.* at Column 3, lines 46–52 and Column 4, lines 12–17. If the operator's access is validated, then a check is made for any policies that further control the operator's access. *Id.* at lines 33–35. The core then creates system-independent certificates that allow the operator to obtain secure access to other devices. *Id.* at Column 6, lines 3–11. A "super user" status can be provided. *Id.* at Column 9, lines 63–67. Once the certificates are created, they are securely reproduced at each different system accessed by the user by "mimicking" the user using key pair validation for security. Column 11, lines 30–42. The '829 patent thus discloses methods and systems to enable an operator of diverse computer systems secure access to those systems using a single authorization from a console.

However, the '829 patent does not show or suggest the unique combinations of elements enumerated above for the pending claims. In particular, the '829 patent is completely silent about how the certificates are evaluated.

Thus, with respect to pending claims 1–8, the '829 patent does not show or suggest the unique elements of: identifying a set of principals associated with a group of certificates; initializing a state associated with each principal; evaluating a certificate at least partly as a function of the state associated with one or more of the principals; updating the state of one or more of the principals if the result of the evaluation indicates that the state of a principal should be changed; and repeating such evaluating and updating until a fixpoint is reached or until a predefined principal is found to authorize the request.

Regarding claim 9, the '829 patent does not show or suggest the unique elements of: means for identifying a root principal from whom authorization is needed in order to grant a request; means for performing at least a portion of a least fixpoint computation over certificates to determine whether the root principal has authorized the requesting principal to access the piece of electronic content or processing resource; and means for granting access to the electronic content or processing resource if the least fixpoint computation indicates that the root principal has authorized such access.

Regarding claims 10–16, the '829 patent does not show or suggest the unique element of a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by performing least fixpoint computations using digital certificates.

Regarding claims 17–20, the '829 patent does not show or suggest the unique elements of: expressing authorizations using a structure that satisfies certain predefined properties; expressing each certificate as a function, wherein each function possesses one or more properties sufficient to ensure that a set of authorizations will have a fixpoint; computing a fixpoint of the authorizations, or an approximation thereof; and making a trust management decision using the result of such computations.

The '050 Patent

The '050 patent describes methods and systems for authenticating program classes that are downloaded to a computer for execution. Briefly, the '050 patent describes a trust manager that authenticates each class prior to execution. *See, e.g.,* Column 3 at lines 34–38. The trust manager examines a policy file that includes data structures defining security policies of the user system, a certificate repository for storing a plurality of certificates, and a certificate being a data record which is digitally signed and which certifies claims relevant to a security evaluation. *Id.* at lines 46–50. A code examiner analyzes the portion of code to determine potential resource use by the portion of code being examined; and a trust evaluator evaluates the certificate requirements of that portion of code based on the policy rules extracted from the policy file and the potential resource use specified by the code examiner. *Id.* The certificates and policies can be in a hierarchical form. *See* Abstract. The certificate includes one or more claims (*i.e.,* statements made by a claimant, *id.* at Column 4 at line 44), which are "data structure[s] defining a policy of [sic] assertions about a class, package of classes, or an entity to be trusted or not trusted." *Id.* at lines 43–45. An assertion is a statement of trust in a claimant or class. *Id.* at Column 4, lines 41–59. When classes are loaded into a computer, the trust manager reviews the associated certificates to identify the claims about the code contained therein and "strings together" the claims until a "proof" is obtained that the code can be trusted. *Id.* at Column 6, lines 52–65. Often "proof" is obtained when a policy claim is reached that does not require proof. *Id.* at lines 64–65. The trust manager searches along various claim paths to reach a determination, but there is no guarantee that such a chain exists; so the trust manager may terminate its search after a set limit. *Id.* at Column 9 at lines 12–20.

Thus, while the '050 patent describes methods and systems for authenticating code before execution, it does not overcome the deficiencies enumerated above with respect to the '829 patent. In particular, the '050 does not show or suggest any of the above-recited unique claim elements, and especially the unique claim elements of a fixpoint computation or the identification of principals and updating their status.

In sum, Applicants respectfully submit that the cited art fails to show or suggest the claimed invention, either individually or in combination, as each of the '829 and '050 patents fail to show or suggest the elements of the pending claims without impermissible hindsight. As noted in detail above, the '829 patent fails to show or suggest many of the elements recited in the pending claims, especially the unique elements of using fixpoint computations and updating the states of the principals. Instead, the '829 patent discloses merely the use of key pair authentication to validate user access rights. Such validation schemes do not require or even suggest the use of fixpoint computations and updating the states of principals. The '050 patent does not overcome the deficiencies of the '829 patent, since the '050 patent also fails to show or suggest using fixpoint computations and updating the states of the principals.

The Applicants respectfully submit that the Examiner has interpreted the various elements cited from the '829 and '050 patents in support of the rejections using impermissible hindsight from the present application to supply the crucial elements where each of those patents is silent. For example, regarding the Examiner's comments concerning claim 1 and its dependents (*i.e.,* claims 1–8), Office Action mailed 17 February 2005 at pages 2–3, the Applicants respectfully submit that none of the cited Figure elements or their associated text show or suggest identifying or updating the states of principals. Such details are provided only in the present application.

The Applicants respectfully submit that fixpoint calculations are not shown or suggested in the cited art; and that the Examiner has used impermissible hindsight to support this rejection. In fact, the Examiner admits that the '829 patent "does not explicitly mention . . . repeating [the claimed] evaluating and updating steps until a fixpoint is reached or until a predefined principal is found to authorize the request". However, the Examiner does not provide any indication where the missing element can be found in the prior art, especially in the cited '050 patent. Moreover, the Examiner appears to make the contradictory assertion that the '829 patent *does* disclose fixpoint calculations. *Id.* at page 8. The Applicants respectfully submit that fixpoint calculations are not shown or suggested in the cited art; and that the Examiner has used impermissible hindsight to support these rejections.

Thus, the Applicants respectfully request that the Examiner withdraw the rejections of claims 1–8.

The Examiner appears to have applied analogous arguments to the rejections of claims 9–17; so, for the reasons provided with respect claims 1–8, the Applicants respectfully request that the Examiner withdraw the rejections of claims 9–17 as the cited art fails to show or suggest (alone or in combination) the claimed element of a fixpoint computation.

Regarding claims 18–20, the Applicants respectfully note those claims also include the unique limitation of a fixpoint computation; and so are patentable over the cited art for at least that reason. However, regarding the Examiner's assertion that Figure 3 of the '829 patent "represents a lattice structure" as recited in claims 18 and 20, Office Action mailed 17 February 2005 at page 9, the Applicants respectfully submit that Figure 3 of the '829 patent merely illustrates a data structure for a single certificate, ’829 patent at Column 2, line 51, and has no relation whatsoever to a lattice that represents the authorizations granted by the principals as claimed. *See* Specification at paragraph [0013] and claim 18.

Regarding claim 19, again the Applicants respectfully point out that claim is patentable for at least the reason of including a fixpoint computation. However, regarding the Examiner’s assertion that the ’829 patent discloses using a monotonic function, the Applicants respectfully submit that no such showing or suggestion is made in the ’829 patent; and that merely comparing usernames and group membership information does not demonstrate a monotonic function.

Thus, one of skill would not be lead to the characterizations offered by the Examiner without the use of impermissible hindsight from the present application. The Applicants respectfully request that the Examiner withdraw the rejections of claims 1–20.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that the pending claims are in allowable form, and respectfully request reconsideration and timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: August 16, 2005

By:____________________
Andrew B. Schwaab
Reg. No. 38,611

Finnegan, Henderson, Farabow
Garrett & Dunner, L.L.P.
901 New York Ave., N.W.
Washington, D.C. 20001
Attorney direct (650) 849-6643